Scaling Effects on Federated Learning Robustness Against Adversarial Poisoning in IoT

Assignee Research

May 31, 2026

Abstract

This report synthesises findings from 1 peer-reviewed paper addressing the following research question: What is the impact of model scaling on the robustness of federated learning systems against adversarial poisoning attacks in IoT security applications. Federated learning (FL) is a privacypreserving method for shortterm load forecasting in energy networks. However, current defense mechanisms against adversarial attacks often depend on supplementary machine learning frameworks, such as anomaly detection models or. 12 claims were extracted from source literature; 7 were independently verified against retrieved documents. An automated multi-reviewer quality assessment produced a score of 6.7/10. This report is a machine-generated literature synthesis and does not constitute original research.

1 Introduction

This paper examines: Trustworthy Distributed Load Forecasting in ResourceLimited Smart Grids and Buildings via Random Layer Aggregation. Research question: What is the impact of model scaling on the robustness of federated learning systems against adversarial poisoning attacks in IoT security applications?.

2 Methodology

Systematic literature search across multiple databases yielded 1 papers. Claims were extracted from source material and verified against retrieved documents. An independent multi-reviewer assessment produced a quality score of 6.7/10.

3 Results

1 papers retrieved. 12 claims extracted; 7 independently verified. Quality review score: 6.7/10.

4 Limitations

This report is a machine-generated literature synthesis and does not constitute original research. Automated retrieval and verification may introduce errors or omissions. Review scores reflect automated assessment, not human peer review. Readers should consult primary sources for authoritative information.

5 Extracted Claims

Claim	Verified	Confidence
Current defense mechanisms against adversarial attacks in federated learning often depend on supplementary machine learn	✓	0.31
Supplementary machine learning frameworks for adversarial defense add significant computational overhead to edge devices	✓	0.24
FedRLA aggregates only one randomly chosen neural network layer per communication round.	✓	0.19
FedRLA reduces attack surfaces by 66% compared to full-model aggregation (FedAvg).	✓	0.24
Using 8-bit quantization, FedRLA cuts data transmission by 92.97% without accuracy loss.	✓	0.24
FedRLA achieves a Mean Absolute Error (MAE) of 0.08 kWh compared to FedAvg's 0.076 kWh.	×	0.15
Under four model poisoning attacks, FedRLA reduces forecasting errors by 19%–35% compared to FedAvg.	✓	0.25
FedRLA uses 24% less CPU than frameworks such as FedProx.	×	0.15
FedRLA uses 13% less memory than frameworks such as FedProx.	×	0.15
FedRLA trains 58% faster than frameworks such as FedProx.	×	0.09
FedRLA achieves a communication efficiency of 0.195 MB per round.	✓	0.15
FedRLA maintains an adversarial robustness with MAE $\leq$ 0.11 kWh under epsilon = 0.2 Differential Privacy.	×	0.14

References

- https://www.semanticscholar.org/paper/631f733ae355e2535785080aa27aa106f314742f